IJMS 11 (SPECIAL ISSUE), 63-78 (2004)

UTILIZATION OF SUBNETWORKS THROUGH DISTRIBUTED GATEWAY IN LAN ENVIRONMENT

AHMAD BASRI HASHIM
ROSHIDI DIN
MD ZAHIR MAT CHA
AZMI MD SAMAN
Faculty of Information Technology
Universiti Utara Malaysia

ABSTRACT

It is a globally accepted fact that there is a significant increase in the use of Internet in a local area network (LAN) environment. Whilst the reliance (dependence) on the costly, and difficult to maintain, hardware and software brings about problems for organizations with small budget, the full utilization of networks is questionable, for example, at schools and colleges where server failure consistently occurs that leads toward inability to access the Internet. To address issues relating to this matter, this paper discusses on the viable alternative of IP masquerading that allows the interconnection of subnetworks and distribution of gateways in a multiple internal LAN environment. For the server which acts as a gateway to the Internet, an IP masquerading distribution based on Linux is used. A distributed gateway based on alternative routes to other gateways in different sub networks will minimize disconnections. The situation will ensure reliable and continuous connection through alternative sub networks in the event of a connection failure in adjoining sub-network. This results in a reliable and cheaper LAN-Internet connection through the IP masquerading servers as an alternative to proxy server software. It also ensures reliable and continuous Internet connection through an alternative sub network in the event of a connection failure in an adjoining sub network.

ABSTRAK

Memang tidak dapat dinafikan bahawa terdapat peningkatan ketara penggunaan Internet dalam persekitaran rangkaian kawasan setempat. Pergantungan semasa kepada perkakasan dan perisian yang mahal dan sukar *untuk diselenggara menimbulkan masalah kepada organisasi yang mempunyai sumber kewangan yang terhad; sebagai contoh sekolah dan kolej yang kerap kali menghadapi masalah kegagalan pelayan dan akhirnya menyumbang kepada kegagalan capaian ke Internet. Justeru, artikel ini membincangkan alternatif penyelesaian menggunakan 'IP masquerading' yang membolehkan sambungan dalaman dibuat kepada subrangkaian dan pengagihan get laluan dalam pelbagai persekitaran rangkaian setempat. Bagi pelayan yang bertindak sebagai get laluan kepada Internet, pengagihan 'IP masquerading' yang berasaskan kepada Linux boleh digunakan. Get laluan yang disebarkan kepada subrangkaian yang lain akan meminimakan masalah terputus hubungan di kalangan pengguna. Situasi seperti ini akan memastikan sambungan ke Internet dapat dibuat secara berterusan dan efisien walaupun dalam keadaan sambungan yang terputus dalam suatu subrangkaian. Kajian ini bertujuan untuk menawarkan sambungan 'LAN-Internet' secara lebih selamat dan murah menerusi pelayan 'IP masquerading' sebagai alternatif kepada perisian pelayan proksi dan memastikan hubungan ke Internet sentiasa berterusan apabila berlaku terputus hubungan dalam suatu subrangkaian.*

INTRODUCTION

Most wired organizations rely on access to the Internet for email and web access. Networked PCs require access via the local area network (LAN) rather than through dedicated modems and telephone line connection. Splitting a network into two separate domains will benefit each sub- network with a lower traffic load. A local Ethernet bridge or router can facilitate connection between two sub-networks where bridge remembers the location of sub network computers. A computer can send packets to another computer within the same part of network bridge and will not pass to other parts of a network. This helps reduce traffic within and between different parts of network.

In most small organizations, a sub network is connected to the Internet through a single gateway. The drawback is that all client machines are automatically cut off from the Internet in the event the gateway, either in the form of proxy servers, or IP masquerading servers, breaks down. Ideally, connectivity within the same part of network can be maintained if IP masquerading takes the role of server by direct connection among clients. As Linux is developed using an open and distributed model, instead of a closed and centralized model like most other softwares, the latest development version is always released to the public so that anybody can use it. The result is that whenever a version with new functions is released, it almost always contains bugs, but it also results in a very rapid development so that the bugs are found and corrected quickly (Cornes, 1997).

IP masquerade is a networking feature in Linux. If a Linux host is connected to the Internet with IP masquerade enabled, then client machines connected to it can reach the Internet as well. IP masquerade allows connection through alternative gateways (other Linux hosts connected to the Internet) in case there is a connection failure in the gateway. The presence of a bridge or router within this set up will not only reduce traffic in a sub network but can also help divert Internet connection to an alternative gateway, ensuring utilization of sub networks.

Many computer labs, for examples in schools and teacher training colleges, use LAN connections and access the Internet through an Internet Service Provider (ISP). Ideally, LANs should rely on both hardware and software solutions, however there are some that only rely on the hardware solution, i.e. routers and Internet sharing, and some rely on software solution and proxy server software that are available in the market. Whilst the expensive hardware solutions is a problem to organizations with small budgets, the cheap software solutions consistently face the problem of network disconnectivity. Thus, the alternative connectivity using IP masquerade, can provide the last alternative to continuous connectivity with affordable cost.

Furthermore, any applications that users want to use on the PC, like Netscape, some telnet and file transfer protocol (FTP) clients must have proxy server support. One disadvantage is that in order to achieve a connection via a proxy server, the client software must be changed to support the proxy service. For example, to connect to a telnet server over a proxy, the users first have to be authenticated by the proxy server then by the destination telnet server (Murhammer & Martin, 1998).

The major difference between a Masq and proxy server is that Masq servers do not need any configuration changes to the client machines. Just configure them to use the Linux box as their default gateway (Roth, 2000). Unlike proxy servers, IP Masq servers do not need any configuration changes to the client machines. In addition Masq servers require minimal hardware resources (Roth, 2000). Internet protocol masquerading (IP Masq) does not require any such special application support.

Client machines using Windows 2000 as the operating system (OS) can access the Internet using the Linux host as the gateway. Windows

2000 also provides features such as allowing client machines to access alternative Domain Name Systems (DNS). This will enable a client machine in one sub network to access a Linux host gateway in another sub network in the event of a connection failure in the first gateway. Thus, utilization of two interconnected distinct sub networks, each connected to the Internet via a Linux gateway can again be realized.

Many computer labs in learning institutions use PCs based on the Intel microprocessor. These PCs usually use networks which are Ethernet based. The networks are mostly constructed on a lab by lab basis. This deprives users in one computer lab from utilizing applications and other utilities like Internet connection which are available from other labs. Users should be given alternative routes, especially in the issue of access to the Internet.

Sub networks can be connected using an Ethernet bridge or router. To make clear that the total communications facility consist of multiple networks, the constituent networks are referred to as sub networks. A network access protocol, such as Ethernet logic, is used to connect a computer to a sub network. This protocol enables the host to send data across the sub network to another host or, in the case of a host on another sub network, to a router (Stallings, 1997). Most of these devices that are available in the market are costly. A cheaper alternative, using a software oriented approach would help reduce costs.

While there are several solutions available for LAN-Internet connection in the market, cost has always been a major issue. Small organizations including schools and colleges have very limited budgets to purchase the necessary software and hardware.

This study involves two Ethernet based sub networks located in two adjoining computer labs. The two labs are separated by a distance of about 30 meters between the nearest PCs. Machines used are x86 and compatibles. For Internet connection, two 56kpbs modems with public services telephone network (PSTN) connections are used. Each gateway were installed with Linux IP masquerading as the server. The study looks at the sub networks from the following angles:

1. Internet access is based on dial up PSTN connections. This project is concerned with common Internet services like the world wide web, ftp, telnet ting, etc.

2. cost reduction is viewed from the server perspective. The use of IP masquerading on the server is viewed as an alternative to

proxy software based servers and this will show a vast reduction in costs.

3. interconnection of sub networks is based on and restricted to two adjoining sub LANs. Sub networks will be connected based on routing.

METHODOLOGY

The study was conducted by using the following methods:

- choosing a suitable IP Masquerading software
- setting up and configuring a LAN Internet gateway
- interconnecting sub LANs for access to the Internet
- ensuring a continuous Internet connection in all sub LANs

There are few changes to the current LAN Internet connection set up, i.e using the proxy server approach. Changes made to client machines are minimal. The only major change is the computer server which utilizes the routing approach. A comparison of the proxy server model and the IP masquerading model are shown in Figure 1 and Figure 2.

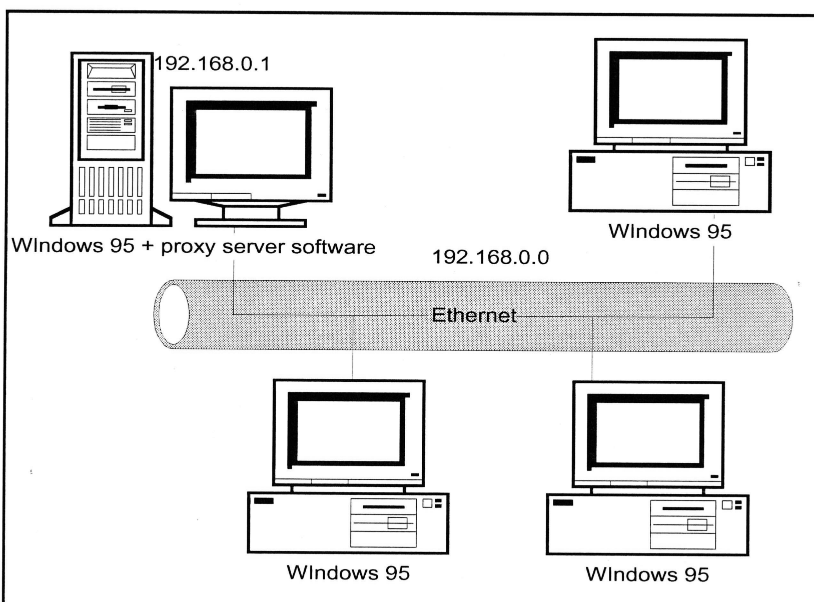

Figure 1
Existing Computer Lab Model

The minimum requirements for the gateway includes:

- CPU - any 386 or better
- RAM - min (with swap) 6 MB, normal 8 MB, recommended 16 MB
- FDD - 1.44 MB
- HDD - not required for 8-16 MB RAM system, but recommended.
- Ethernet adapter(s) - 3COM509, 3COM595, 3COM905, Realtek NE2000 compatible, Realtek NE2000 PCI compatible, ISA/PCI NE2000 compatible supported out of box.
- Modem(s) - most modems except win modems will work with FREESCO.

The LAN was created by direct connection of computers using:

- 10base2 cables
- Network terminators
- Network interface cards (NIC), 1 per networked computer
- Server

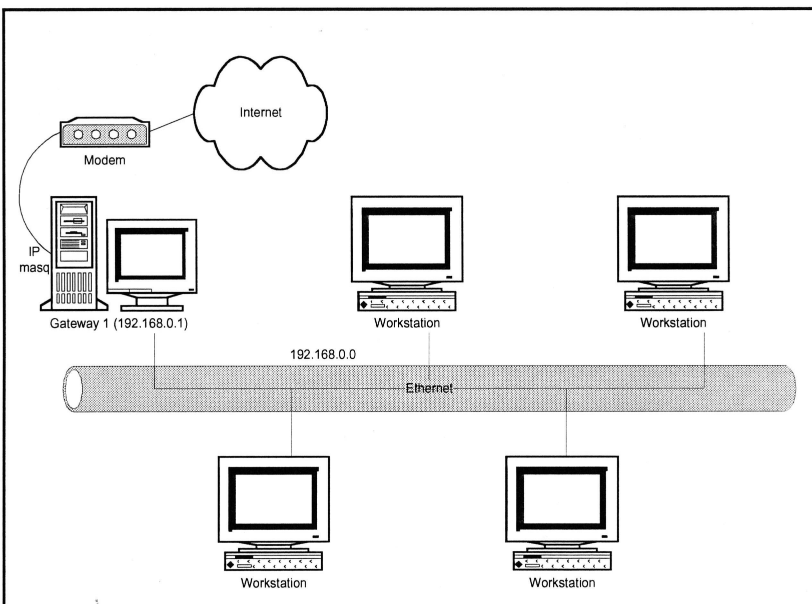

Figure 2
An Example of Computer Lab Model Using the
IP Masquerading Method

For this study, ISA NE2000 compatible NICs are used. For Internet access, dial up lines with 56 kpbs modems were used. While leased

and not always readily available, the telephone
everywhere. So, dial-up connection over tel-
osen for connecting LANs to Internet. Point to
s used over voice phone lines.

ection Through the Use of IP Masquerading

f the above, the following has to be resolved.

i.e. gateway 1 for network 192.168.0.0 and gate-
k 192.168.10.0.

client machines in networks 192.168.0.0 and

um 133 PC, with 41MB HDD, 1.44 MB FDD and
l for gateway 1 of the first network and for gate-
ised is similar to gateway 1. DNS server is set as
y 1 and for gateway 2, the DNS server is set as
machines in both networks, configurations were
sing was automatic because DHCP was enabled.

Through an Alternative Sub network

f both networks 192.168.0.0 and 192.168.10.0 in
e project, there are two practical choices, namely:

g was used. Routers can be used to interconnect
h a way that the traffic generated on one LAN is
e traffic generated on the other LAN (Walrand,
nterface cards (NIC) were installed to facilitate
sub LANs. Thus both gateways not only pro-
rnet but also act as internal routers interconnect-

he project interconnects two sub LANs as illus-

clients on network 192.168.0.0 to also access the
vay 2 and clients on network 192.168.10.0 to ac-

cess the Internet through gateway 1 in the event of a connection failure in either network. The set up for both gateways is now different from the first phase where the sub LANs were separated. The IP addresses of the first and second network interfaces, respectively, in gateway 1 are 192.168.0.1 and 192.168.10.2 whereas for gateway 2, the IP addresses are 192.168.10.1 and 192.168.0.2.

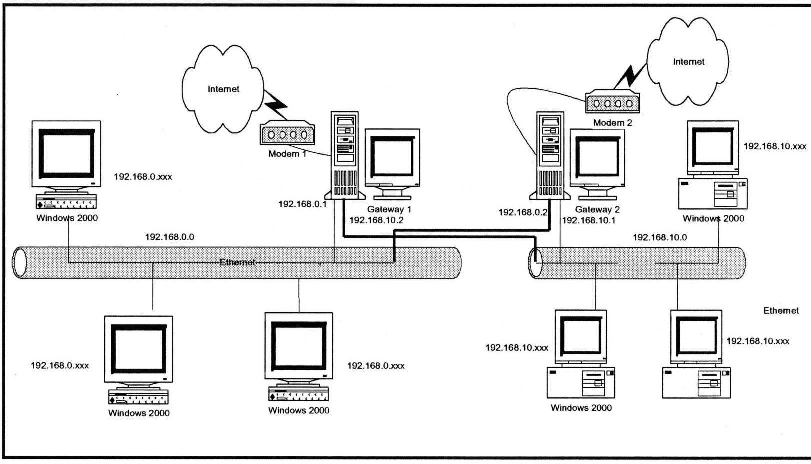

Figure 3
An Example of Two Interconnected
Sub LANs Using IP Masquerading

The client machines on both sub networks were configured so that each PC on each sub network is able to access the Internet either from gateway 1 or gateway 2. With Windows 2000 installed on all client machines, network 192.168.0.0 was configured with the preferred DNS server being 192.168.0.1 and the alternate DNS server is 192.168.0.2. Client machines on network 192.168.10.0 were similarly configured with the preferred DNS server now being 192.168.10.1 and alternate DNS server is 192.168.10.2.

Since all internal IP masqueraded machines must not have official Internet assigned addressees, there must be specific and accepted way to allocate addresses to the machines without conflicting with anyone else's Internet addresses. *RFC 1918* is the official document on which IP addresses are to be used on a non-connected or private network. There are 3 blocks of numbers set aside specifically for this purpose. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

The first block is referred as 24-bit block, the second as 20-bit block, and to the third as 16-bit block. The first block is a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 255 contiguous class C network numbers. For this project, the preference is to use the 192.168.0.0 network with a 255.255.255.0 Class-C subnet mask for the first sub LAN and 192.168.10.0 network with a 255.255.255.0 Class-C subnet mask for the second sub LAN. 192.168.0.1 and 192.168.10.1 are the internal gateways to get out to the external network. 192.168.0.0, 192.168.10.0 and 192.168.0.255, 192.168.10.255 are the network and broadcast addresses respectively (these addresses are reserved). These addresses are avoided to enable the network to work properly.

DNS server converts Internet addresses between human readable form (example: www.abc.net) and computer readable form (example: 195.2.83.113) and back. This local caching DNS server can reduce traffic between the local network and Internet Service Provider (ISP) and increase speed of connections to servers on the internet (Gaskin, 1999). To set up a DNS server we have to know the ISP DNS address. For this project, since the ISP used is the one provided by TMNet, the ISP DNS address is 202.188.0.133.

DHCP server provides automatic configurations of the local networks computers. It makes the job of the network administrators easier. Every computer on the network must have its own IP address and it must also know the DNS address and gateway. The DHCP server supplies every computer on the network with this information (Gaskin, 1999). For this project, the DHCP is enabled for configuration on the local clients and the DHCP server will do the rest, otherwise we have to enter all these addresses manually.

We can have full access to the gateway via telnet connection. Unlike http control service in the Freesco web panel, it does not have any restrictions and we can edit the config files from the workstation via telnet connection.

Another component required to use Internet resources is application software for workstations, which are IBM PCs compatible with the

MS Windows 2000 operating system. This version of MS Windows is better equipped with Internet client software, in particular Internet Explorer compared to previous versions.

The other applications covered in each workstation have at least the following Internet services:

- Telnet (client with a VT100 / VT220 emulation).
- FTP (client with graphical user interface).
- WWW (Netscape Navigator version 4.0 onwards besides Windows 2000 built in Internet Explorer).

Helper applications were also included to support:

- MPEG audio and video files.
- PostScript files.
- PDF (Portable Document Format) files.
- Compressed files (ZIP, Z, GZ, TAR)

The majority of the above applications are free, some of them are low cost shareware.

DISCUSSION AND FINDINGS

This project looks at the development of computer lab models based on the IP masquerading LAN Internet gateway as well as the interconnection of two sub LANs for connection to the Internet.

LAN-Internet Connection Through the Use of IP Masquerading Servers

Configuration of client machines were done without any problems. For the first network (i.e: 192.168.0.0), each client machine was able to detect each other using the built in Packet Internet Groper (PING) program for Windows 2000. With Dynamic Host Configuration Protocol (DHCP) enabled, each client on the network have their own assigned IP addresses. The same is true for the second network, 192.168.10.0. Unlike proxy servers, through IP masquerading there is no need for any configuration of browser programs on client machines for access to the Internet.

For server set up, the freesco distribution was downloaded in 3 minutes and initially installed on a 1.44 MB floppy disk. Once booted from the floppy, it was copied and moved to the hard disk without any problems. This was to make use of swap file from the hard disk to increase amount of memory. Setting up the gateway from the hard disk in network 192.168.0.0 was done without any problems. The modem and the NIC were also detected without many problems. The same was observed for network 192.168.10.0.

Once the freesco gateways at 192.168.0.1 and 192.168.10.1 were up and running, clients in each network were able to utilize the web control panel. However this was restricted to trusted users with password access provided by the administrator. Figure 4 shows an example of a web control panel screen as viewed from client in network 192.168.0.0.

Once the network setup enabled the PCs to communicate and gateways were properly configured, web access and other basic Internet services were readily available. This shows that a basic PC with minimal hardware and software resources can be a reliable LAN Internet server, thus drastically reducing costs as compared to a proxy software server based approach. The following figure (Figure 4) shows the screen example of freesco web control panel.

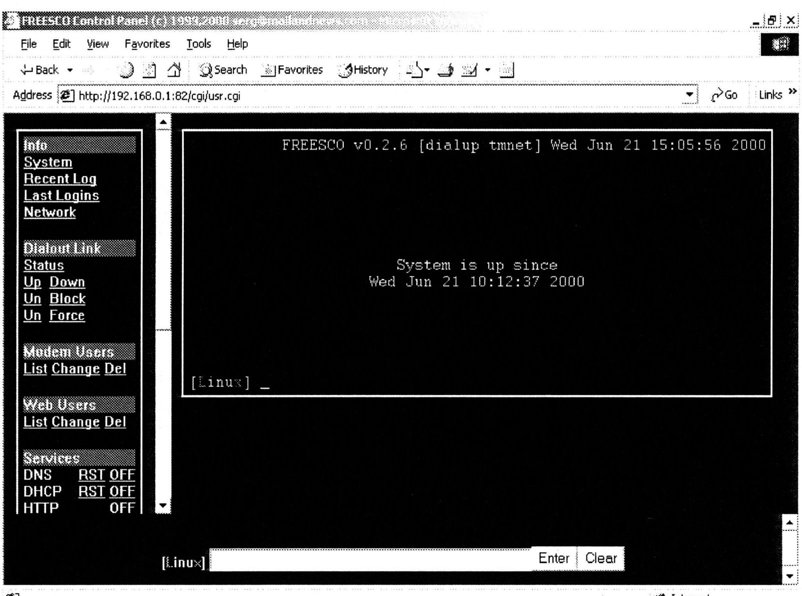

Figure 4
Freesco Web Control Panel

Continuous Internet Connection Through An Alternative Sub-Network

Freesco 2.6 was installed in both servers without problems except for the detection of the two NICs on each server for alternative Internet connections. However, this was eventually overcome by first checking the BIOS and making sure there was no conflict with an existing serial port or IRQ. After checking the file var/log/log it was found that the names eth0 and eth1 had been swapped. The alternative was to swap the interface names in advanced setup in freesco through options 72 and 73 from memory, change "first network interface" to eth1 and the second to eth0. With the gateways also functioning as internal routers in each network, client machines in each network were able to communicate with each other through these routers.

Once the network setup enabled the PCs to communicate and gateways were properly configured, access to the Internet was not a problem. Both gateways in networks 192.168.0.0 and 192.168.10.0 were very stable especially in low traffic. Heavy traffic affected access speeds, especially when both computer labs, consisting of 20 PCs each, were fully occupied although this situation of maximum use of Internet in both sub LANs was rare. However, speed problems were negligible for basic use such as surfing the web.

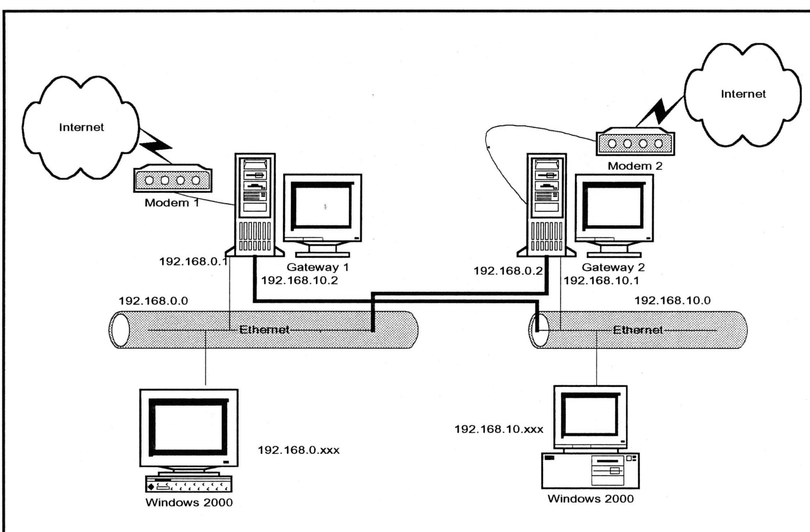

Figure 5
Distributed Gateway

Table 1
Internet Access in Sub Networks

Modem 1	Modem 2	Clients in network	Internet
On	Off	192.168.0.0 and 192.168.10.0	On
Off	On	192.168.0.0 and 192.168.10.0	On

As shown in Table 1 (refer also Figure 5), it was also found that a disconnection of modem in one sub LAN, did not affect access to the Internet as long as connection in the other sub LAN was secure. This conforms with the findings in the paper 'Designing Large-Scale IP Internet works' from Cisco Systems technology information (2000) that most networks are designed with multiple paths so there are alternatives in case a failure occurs. Other factors beyond control, for example PSTN line disturbances and TMnet server problems affected Internet access.

Suggestion for a Computer Lab Model

Computer labs with Internet access based on IP masquerading can be a viable alternative to those based on the current set up of proxy servers mostly using Ethernet networks and dial up modems on PSTN telephone lines. The presence of distributed gateways also ensures broken access to the Internet is kept to a minimum. This is an important feature in IP masquerading which provides an option for alternate gateways where this is not available in the software of the proxy server. The server set up, using the freesco 2.6 distribution is not too complex and if suitable hardware is chosen, any problems that may arise can be easily overcome. Although client PCs need not necessarily be Windows based, Windows 2000 was maintained in the PCs as it was originally installed in the previous proxy server based network. The Ethernet wired with 10 base2 coaxial cables is the current network design with very minor changes being made for this project. The only alterations made were for the purpose of interconnection of sub LANs using the two NICs installed in both gateways.

Computer labs today need to be networked and have access to the Internet. Unfortunately, this has become a costly affair, more so for schools and colleges with very limited budget. The increasing popularity of Linux as the alternative to Windows could be a blessing for these types of organizations. In line with the Malaysian National Information Technology Council's proposal (*Computimes*, August 7, 2000) to create equitable access to information among the people, the further decrease on hardware and software costs can be a contributing factor towards realizing this goal and hence address the digital divide among the people. The recent encouraging breakthrough in the development of molecular electronics (*IN-TECH*, August 1, 2000) which promises to revolutionize computer processor speed with tremendous cost savings is another positive development. Used 486 machines can be purchased at minimal cost these days. These machines, with some extra RAM and hard disk space added on, are enough for Linux to run on.

Suggestion for Servers:

1. Freesco IP masquerading server using Pentium 100 MHz.
2. Print servers based on freesco IP masquerading using 486DX-100 MHz machines.

Suggestion for Clients:

1. 86DX-100 MHz machines using the Linux OS.
2. Office suite based on the Linux OS, for example Staroffice, which is another free application.
3. For Internet browsing, Netscape for Linux.

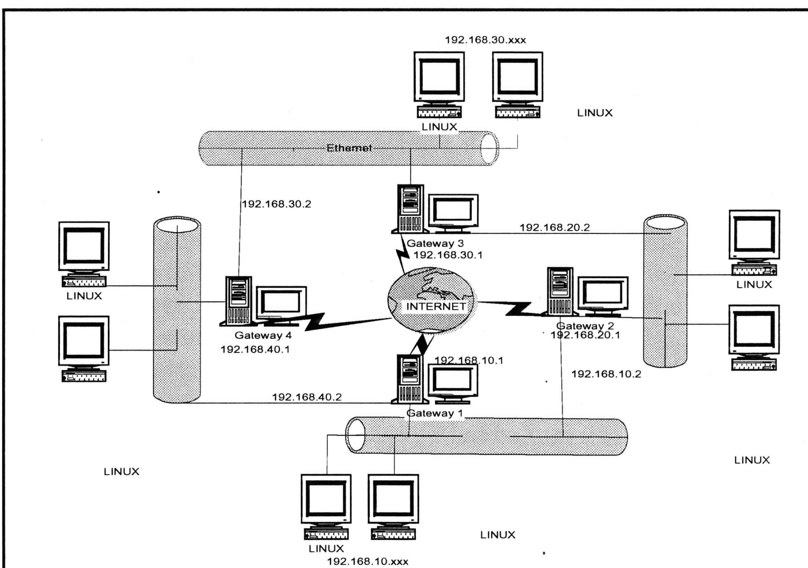

Figure 6
Distributed Gateway of Sub Networks in a Linux Environment

A possible design of interconnected computer of sub networks in a Linux environment is shown in the Figure 6 .

CONCLUSION

Freesco was developed in the open source tradition as an alternative to routing products offered by the more established networking hardware solution providers. This provides management one way to decrease expenses.

This research is far from complete in terms of providing a cost effective solution in the utilization of sub networks for Internet access but the free and open source environment of Linux of which this project's IP masquerading is based on, can be further exploited to address issues such as bandwidth. If this can be overcome it will hopefully increase user satisfaction, particularly access to the Internet in a LAN environment. Coupled with the potential of the increased use of diskless computers and the future development of molecular electronics, further cost reduction is possible.

Implementing a functional internet work is no simple task. Many challenges must be faced in areas like connectivity, reliability, network management and flexibility. Each area is important in establishing an efficient and effective internet work. Another essential consideration is reliable service which must be maintained in any internet work. Individual users and entire organizations depend on consistent, reliable access to network resources. Furthermore, network management must provide centralized support and troubleshooting capabilities in an internet work. Configuration, security, performance, and other issues must be adequately addressed for the internet work to function smoothly. Flexibility, the final concern, is necessary for network expansion and new applications and services, among other factors.

REFERENCES

Computimes (2000, August 7). Creating an equitable access to information among the people.

Cornes, P.(1997). *The linux A-Z*. Hertfordshire: Prentice Hall.

Gaskin, E. (1999). *Mastering netware 5*. Alameda, CA: Network Press

IN-TECH (2000, July 18). *The Star*.

Murhammer, W. & Martin (1998). *TCP/IP tutorial and technical overview*.

Upper Saddle River, New Jersey: Prentice Hall.
Roth, S.(2000). *Proxies vs. NAT*. Retrieved June 15, 2000 from http://www.homepclan.com/proxynat. htm/
Stallings, W.(1997). *Local and metropolitan area networks*. Upper Sadle River, New Jersey: Prentice Hall.
Walrand, J.(1998). *Communication network: A first course*. San Francisco: McGraw Hill.